
CSUTAK ZSOLT

**SZÉP ÚJ VILÁG, AVAGY A KIBERTÉR
ÉS A MESTERSÉGES INTELLIGENCIA KORÁNAK
ÚJ KIHÍVÁSAI**

*„ágyúk és golyók... az igazi fegyverek,
nem egy laptop”¹*

A kiberkor kezdetén

Közhelyszerű megállapítás, hogy aszimmetrikusan fejlődő posztmodern korban élünk, amelyben a nemzetközi kapcsolatokat a rendezett anarchia állapota jellemzi, és a hatalmi színpadon egy amerikai szuperhatalom mellett kibontakozó multilaterális erőközpontú rivalizálás zajlik. A feltörekvő ázsiai hatalmak, régi magállamok, mint Kína, India, Oroszország vagy akár még a latorállamként számon tartott Észak-Korea is próbálnak minél nagyobb erő- és életteret kiharcolni maguknak a világpolitika és -gazdaság irányításában, amihez változatos eszközöket kell alkalmazniuk.

A közismert hadművészeti clausewitzi tétel, miszerint a háború a politika meghosszabbítása más eszközökkel, illetve erőszakos érdekérvényesítési eszköz,² részben helytálló tétel még a 21. század posztmodern módon ellentmondásos világában is, hiszen napjaink háborús és számos egyéb jellegű, fegyveres konfliktusai a maguk anakronisztikus módján, de mind ez irányba mutatnak. Sok elemző szerint már zajlik a harmadik világháború, csak más, merőben új eszközökkel és teljesen új hadszíntéren vívják, ellenben ugyanazon hagyományos politikai, gazdasági, továbbá eszmei célok érdekében: gazdasági előnyszerzés, nyersanyag-lelőhelyek, létfontosságú globális kereskedelmi útvonalak, fojtópontok feletti ellenőrzés biztosítása és az információáramlás felügyelete céljából, kiegészülve a vallásos doktrínákkal hangsúlyozott huntingtoni civilizációs szembenállással.

Tanulmányomban központi helyet kap a **kiber** szó és annak különféle alkalmazási módjai a hadtudománytól a modern nyelvészet kontextusáig, különösképpen a **kiberhadviselés** és a kiberbűnözés egyre gyakrabban használt tartalmáig. Ebben a vonatkozásban viszonylag sokszor fogunk találkozni az egyik névadó, Richard A. Clarke³ professzor, veterán washingtoni nemzetbiztonsági elnöki tanácsadó gondolataival, akárcsak neves washingtoni kiberbiztonsági szakértő munkatársai, Robert Knafe és Paul Kurtz meghatározó véleményével, akik szerint

¹ Közkedvelt amerikai haditengerész bölcsesség volt az 1990-es években, egészen a 2003. évi második Öböl-háborúig, amikor megalakultak az amerikai haditengerészet és légierő kiberosztagai.

CLARKE, Richard A. – KNAKE, Robert K.: Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins, New York, 2010. p. 19.

² Clausewitz, Carl von: A háborúról. Zrínyi Kiadó, Budapest, 2013. pp. 39–45.

³ Bestseller műve az új típusú kiberháborúról: CLARKE, Richard A. – KNAKE, Robert K.: Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins, New York, 2010.

a 21. század fő konfliktusai – állami és nem állami szereplők között egyaránt – elsősorban az úgynevezett kibertérben fognak lezajlani, pontosabban már évek óta zajlanak.⁴

Mielőtt belefognék a fontos terminológiai és fogalmi körülírásba, előljáróban érdekes és hasznos lehet megosztani Clarke professzor egyik jellegzetes és anakronisztikus történetét a klasszikus, vagy amerikai szakzsargonban kinetikus haderőnemi (kinetic hard power) és a posztmodern kiberhadviselés (cyber warfare) közötti nem túl baráti szembenállásról, különbségről. Modern korunk legendás amerikai hadvezérének, Norman Schwarzkopf tábornoknak már az első, 1991-es öbölháború idején javasolták, hogy az iraki légvédelmet és radarrendszert számítógépes programokkal iktassák ki vagy zavarják össze a nagy támadás előtt. Erre ő rezignáltan csak annyit felelt: „*Bombázzuk le azokat, az az igazi! Nyavalyás számítógépekkel nem lehet harcot vívni!*”

Egy évtizeddel később, a második öbölháború előestéjén – vagy Irak lerohanása előtti napon –, 2003. március 19-én közel ötezer magas rangú iraki katonai vezető az iraki vezérkari főnök belső titkos e-mail címéről kapott egy díszes fejléces angol és arab nyelvű üzenetet az Amerikai Egyesült Államok Központi Parancsnokságától, amelyben felszólították őket a passzív ellenállásra, illetve a vezénylésük alatt álló csapataik visszatartására a hamarosan bekövetkező amerikai támadás napján, saját életben maradásuk érdekében. A feltört levelezőrendszer és a mögötte sejtethető kiberfegyver érezhetően és láthatóan is megtette döbbenetes lélektani és morálisan romboló hatását az iraki haderőre az alig hat hétig tartó teljes Szaddám Huszein-rendszer összeomlásának bekövetkeztéig. Számos páncélososztag várta felsorakozva a támadást, csak éppen kezelőszemélyzet nélkül. Az iraki hadsereg és légierő belső elektronikus kommunikációja, az országos radarrendszer és a csapatkoordináció már jó ideje az amerikai légierő kiberparancsnokságának távfelügyelete alatt állt, amely 2003-ban még önállóan nem is igazán létező csoportként működött, de akkor nyerte el igazán létjogosultságát.⁵

Közel két évtized távlatából visszatekintve, a hadtörténészek és a kiberszakértők szerint a második iraki háború volt az első elektronikus vagy kiberhadviselést is alkalmazó nagyméretű konfliktus, habár a 2007-es észtországi, a 2008-as grúziai és az azt követő koreai, amerikai és egyéb célpontok elleni kiberháborús események már minden szempontból jóval magasabb rendű, minőségi és mennyiségi ugrást jelentettek az iraki háborúban alkalmazott technológiákhoz képest. Mindezekről már számos részletes kiberbiztonsági esettanulmány született hazai és külföldi szerzőktől egyaránt, ezért ebben a tanulmányban elsősorban a kibertér és a kiberhadviselés eszmei és technológiai háttérkérdéseire szeretnék fókuszálni.⁶

⁴ CLARKE, Richard A. – KNAKE, Robert K.: *Cyber War: The Next Threat to National Security and What to Do About It*. Harper Collins, New York, 2010. pp. 13–18.

⁵ CLARKE, Richard A. – KNAKE, Robert K.: i. m. p. 12.

⁶ GULYÁS Attila: *Kiberhadviselés észak-koreai módra II*. Szakmai Szemle, XV. évfolyam 4. szám, 2017. december. pp. 30–42.
http://knbsz.gov.hu/hu/letoltes/szsz/2017_4_szam.pdf; letöltés: 2018.03.01.

*„egy áramszünet lehet, hogy csupán áramszünet,
ellenben a kiberhadviselésben már lehet,
hogy egy előzetes katonai csapás része”*
Norton Schwartz tábornok⁷

A „hálózat” fogságában

A legújabb technológiákat és fejlesztéseket bemutató Wired magazin 2014. júliusi számában megjelent Joris Toonders⁸ cikke szerint a 21. század újabb ipari forradalmának korában az új világ olaja nem más, mint az adat. A holland webmarketing szakértő nagyon találó megállapítása – Mark Getty⁹ internetguru elhíresült bon mot-jának parafrázisaként – a 21. századot leíró metaforák mesterpéldája lehetne, hiszen amennyiben körbetekintünk a dolgok/tárgyak internete uralta világunkban, mindenfelé információfelhőkbe burkolózó embereket és adatokat feldolgozó okos kütyüket láthatunk.

Az előbb említett dolgok internete vagy Internet of Things (a továbbiakban: IoT) a 2017-es állapotok alapján közel 25 milliárd okoseszköz webalapú összekapcsoltságát jelenti az önvezető elektromos autóktól az önjáró metrókocsikon és az automata teherhajókon keresztül az okos szemüvegekig, továbbá ez a szám a megbízható előrejelzések szerint 2025-re elérheti a döbbenetes 75 milliárd interneten összekapcsolt okoseszközt is.¹⁰ Rögtön adódik a jogos kérdés, miszerint ki vagy mi képes felügyelni, irányítani, illetve biztonságos emberbarát működést biztosítani ennek a milliárdnyi okoseszköz számára egy olyan fékezhetetlenül fejlődő, számítógépek uralta világban, ahol a webalapú bűncselekmények és visszaélések száma 2015-ben az Amerikai Egyesült Államokban és az Egyesült Királyságban¹¹ már letaszította trónjáról a szervezett bűnözést és a kábítószer-kereskedelmet?

E rövid terjedelmű írás keretei között kísérletet teszek ilyen és ehhez hasonló kérdések végiggondolására, felvetésére, amelyek tulajdonképpen a nemzetközi rendszer globális biztonságérzetével és meghatározó szakirányú felfogásával foglalkoznak. Lehetőségem szerint a következő átfogó kérdéseket szeretném körbejárni, megvizsgálni, nevezetesen, hogy hol tart az emberiség a számítógép-alapú vagy kibertársadalom és -gazdaság tekintetében; milyen fő

⁷ Norton A. Schwartz tábornoknak tulajdonított mondás, az Amerikai Légierő és a Különleges hadműveleti és kiberhadviselés csoport első parancsnoka.
CLARKE, Richard A. – KNAKE, Robert K.: i. m. p. 25.

⁸ TOONDERS, Joris: Data Is the New Oil of the Digital Economy. Wired, July 2014.
<https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/>; letöltés: 2018.01.25.

⁹ Mark Getty, a híres Getty Images vállalat alapítója szerint „a 21. század olaja nem más, mint a szellemi tulajdon védelme”. GETTY, Mark: Blood and Oil. The Economist, March 2, 2000.
<https://www.economist.com/node/288515>; letöltés: 2018.03.02.

¹⁰ STATISTA 1. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>; letöltés: 2018.01.28.

¹¹ EVANS, Martin – Scott, Patrik: Fraud and cyber crime are now the country's most common offences. The Telegraph, 19 January 2017. <https://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/>; letöltés: 2018.01.29.

veszélyforrások, kiberbiztonsági kockázatok, kihívások léteznek és fejlődhetnek ki a jövőben, illetve a lendületesen fejlődő mesterséges intelligencia (a továbbiakban: MI) milyen optimista vagy talán disztópikus forgatókönyveket rejthet az emberiség számára.

Mielőtt belevágnánk a lehetséges válaszkísérletek taglalásába, fontosnak tartjuk meghatározni a sokat használt, ellenben annál nehezebben megragadható kiber és kibertér fogalmak tartalmi jelentését és használatának kontextusát. Az angol cyber megfelelőjeként a magyar nyelv is honosította a görög eredetű kiber kifejezést,¹² amely köznapiban használatban tulajdonképpen nem egyéb, mint egy tudományos-fantasztikus irodalomból származó **metafora**, amelyet a híres kanadai–amerikai író, William Gibson használt először 1982-ben a számítógép-alapú hálózatok és az ember interaktív virtuális kapcsolatrendszerének leírására.¹³ Napjainkra ez a szimbolikus vagy metaforikus tér szélesebben digitalizálódott, világunk másodlagos valóságává vált, sőt mondhatjuk, hogy az utóbbi évtizedek Z és α generációi számára inkább már az elsődleges realitás tapasztalatát nyújtja, annak minden elképzelhető előnyével és tragikomikus hátrányával együtt. Később még szeretnék behatóbban foglalkozni az emberi mértékkel már szinte követhetetlen sebességgel fejlődő kibervilág kihívásaival, illetve a számítógép-alapú mesterséges intelligencia lehetséges forgatókönyveivel és potenciális veszélyforrásaival, a tanulmány terjedelmének korlátozott keretein belül.

Gibson, akárcsak művelt természettudós és neves sci-fi író társai, mint Clarke, Vinge vagy legfőképp Asimov, a számítógépek uralta világról alkotott elképzeléseiket, illetve a számítástechnika alapját képező adat- és információ-feldolgozás, illetve -áramlás és rendszerbe szervezés ötletét természetesen a kibernetika nevű új tudományágból merítették, amely a második világháborút követően forradalmasította a matematika és a számítástechnika irányvonalát, és egyben a megváltozott paradigmájú világról szóló filozófiai gondolkodást is.

Norbert Wiener 1948-ban közzétett *Cybernetics* című műve útjára indította mondhatni a 20–21. század új alaptudományát, amelyben sajátosan ötvözte a természettudományos matematikai éleslátását, illetve mestere a híres angol matematikus-filozófus, Bertrand Russell mély bölcséleti hatását. Ezen a ponton fontos lehet megjegyezni, hogy a második világháború idején és különösképpen az azt követő hidegháború évtizedeiben szinte minden jelentős tudományos-műszaki felfedezésnek vagy áttörésnek kapcsolódnia kellett a haditechnikához, illetve a gyakorlatiasabb katonai stratégiákhoz – egyrészt biztonságpolitikai másrészt az elérhető pénzügyi és humán erőforrások szempontjából – mind az Amerikai Egyesült Államokban, mind az egykori Szovjetunió globális érdekszférájában egyaránt.

¹² Kibernetész görögül hajó kormányosát jelenti, átértelmezve az információ irányításának, kormányzásának készségére utalva.

KIS János: A régi görögök erköltséinek és szokásainak vagy vallásbéli, polgári, hadi és házi rendtartásainak leírása Eschenburg szerint. Weber Simon Péter nyomdájára, Pozsony, 1809. p. 142.

¹³ Gibson 1982-ben megjelent *Burning Chrome* című novellájában utal erre az összefüggésre, habár a sci-fi brit nagymestere, Arthur C. Clarke 1956-os *A város és a csillagok* című regényében már használt teljesen hasonló leírást, de nem ezzel a kifejezéssel, hanem „virtuális mátrix” illetve a „virtuális valóság” használatával.

GIBSON, William: *Cyberspace*. <http://www.technovelgy.com/ct/content.asp?Bnum53>; letöltés: 2018.02.25.

Természetesen ez alól nem volt kivétel az atom- vagy a kvantumfizika és a kibernetika új tudománya, vagyis Wiener sem, aki többek között a légvédelmi rendszerek működési optimalizálásának számításain is dolgozott Amerikában.¹⁴ A híres Manhattan-terv, a SAGE-program és az ősinترنتet jelölő ARPANET szintén kapcsolódási pontokkal rendelkezhet ehhez a témához és a kibernetika tudományához az okoshálózatok, az ember és a számítógép interakciójának úttörő momentumainak leírásával. Látható módon a kiber elnevezés és a Wiener-féle kibernetika a fogalmi kölcsönzésen túl is rokonítható eszmeiségű, hiszen a kibernetika tudományából, illetve az általa kialakuló újabb tudományágak, mint a játék-, a rendszer- és a hálózatelmélet elképzelései és alapvetései tartalmilag is összekapcsolhatóak.



1. kép. A net egyik modellje Barabási szerint¹⁵

Az említett, új paradigmát képviselő kibernetikai tudományágakban felettébb komoly hozzájárulással büszkélkedhetünk magyar tudós gondolkodóink részéről, hiszen gondoljunk csak Neumann Jánosra, Erdős Pálra, von Bertalanffyra, Hunfalvy Jánosra vagy újabban az erdélyi származású harvardi–budapesti kutató fizikusra, Barabási Albert-Lászlóra, a hálózatok új tudományának vezető kutatójára. Barabási, felhasználva elődjei nagyszerű halmaz- és játékelméleti alapjait, bostoni kutatócsoportjával megpróbálta lemodellezni az emberiség által valaha létrehozott legnagyobb, legösszetettebb és legdinamikusabban fejlődő hálózati rendszert, vagyis az internetet.¹⁶ Megállapításai szerint az interneteshálózat-topológia is hasonló szabályszerűséget mutat, mint a legtöbb ember alkotta óriás szervezet: kapcsolódási csomópontok és redundáns hálózatok gigahálózata, akárcsak a mikrokozmosz a makrokozmosz tükörképe (1. kép). E hálózatmodell segítségével sokkal könnyebben megérthető és áttekinthető a világháló működése és kapcsolódási algoritmusai, amely

¹⁴ Norbert Wiener – Wikipédia szócikk.
https://hu.wikipedia.org/wiki/Norbert_Wiener; letöltés: 2018.01.19.

¹⁵ <https://pbs.twimg.com/media/DNZFrueWkAAKKRU.jpg>; 2018.03.10.

¹⁶ BARABÁSI Albert-László: Behálózva – A hálózatok új tudománya. Helikon Kiadó, Budapest, 2013.

nyilvánvalóan már rég túlnőtte eredeti, 1970-es évekbeli ARPANET-es¹⁷ alkotóinak legvakmerőbb elképzeléseit is. Kifejezetten izgalmas és érdekfeszítő fejlemény Barabási szerint is, hogy híres magyar írónk, Karinthy Frigyes nem túl közismert „hat lépés távolság szabály” elmélete¹⁸ újból bizonyítást nyert az internet és a közösségi hálózatok működésének vizsgálata során.¹⁹

Ismert közhelyeszerű kijelentés szerint, az Amerikából induló információs szupersztráda vagy internet az utóbbi három évtizedben meghódította az egész világot, amely ugyanakkor sajnálatosan egy torz, hamis tükörképet mutat nagyon egyenetlen és aránytalan módon fejlődő világunkról, ahol a közel 8 milliárd földlakó fele egyáltalán nem használ számítógépet és nincs internet-hozzáférése,²⁰ sőt körülbelül 1,5 milliárd emberhez a villanyáram sem jutott még el. A hadtudomány új kedvenc kifejezésével élve aszimmetrikus, mondhatni párhuzamos tér-idősíkú világokban él az emberiség nagy része. Szélsőséges példán érzékeltetve: hasonlítsuk össze a kaliforniai Szilikon-völgy magasan képzett lakóit az afrikai megaváros Lagos szeméttelépén élő milliókkal vagy akár Indonézia, Kongó, Brazília dzsungellakóinak életmódjával, amely sem tudomány-technológiai, sem antropológiai szempontból nem sokat változott az utóbbi évezredben. A világ egyik fele már nem tudja elképzelni hétköznapi életét az internet virtuális valósága és a zsebében lapuló, több ezer alkalmazást nyújtó okoseszköz nélkül, amely ugyanakkor nem kevés veszélyforrást is jelent életükre. A számítógépes rendszerek és az azokat összekötő optikai és tenger alatti kábelek globális hálózata által megvalósult az Isaac Asimov által 1964-ben vizionált globális számítógépes információs adatbázis és tudáskönyvtár,²¹ az önvezető autókkal és a mesterséges intelligencia hétköznapi alkalmazásával együtt. A döbbenetes mértékű napi 7700 petabyte adatforgalmat²² generáló számítógépes világháló eléréséhez csupán két dologra van szüksége egy potenciális felhasználónak: webkapcsolatú számítógépre vagy okoseszközre (hardware) és a kezeléshez szükséges alapkészségekre, úgynevezett digitális írástudásra (software skill). A világ legnagyobb közkönyvtáraként is működő washingtoni Kongresszusi Könyvtár 15 millió kötetes könyvvállományának többszörösét kitevő napi globális internetes adatforgalom figyelésére, ellenőrzésére, szűrésére gyakorlatilag nincs lehetőség vagy mód, csak regionális vagy különleges esetben országos szinten (lásd Észak-Korea esetét vagy a Nagy Kínai Tűzfalat). Az internet és a rajta futó népszerű kezelőprogram, a worldwide web (világháló) atyjai, nevezetesen Vinton Cerf és Tim Berners-Lee sokáig megvalósulni látták nagy álmukat, hogy

¹⁷ ARPANET – Advanced Research Project Agency’s Network. Az amerikai haditengerészeti tudományos kutató ügynöksége, a DARPA által létrehozott egyetemi és katonai számítógépes hálózat az Amerikai Egyesült Államok keleti és nyugati parti számítógépközpontjai között. 1969-től 1983-ig létezett, amikor külvilágtól és létrejött a polgári hálózat, az ősineternet és a katonai hálózat, a MILNET.

¹⁸ Karinthy írta 1929-ben a Láncszemek című novellájában látnoki módon, miszerint bárkit ismerhetünk a világban, hiszen ismerőseink kapcsolatrendszere exponenciálisan behálózhatja az egész világot. A globális internet DNS Root Node csomópontjai, illetve a közösségi háló világhíres celebjai is ugyanígy viselkednek tulajdonképpen, amint Barabási Albert-László bebizonyította 70 évvel később.

¹⁹ BARABÁSI Albert-László: i. m. pp. 34–45.

²⁰ STATISTA 2. Global digital population as of April 2018 (in millions).

<https://www.statista.com/statistics/617136/digital-population-worldwide/>; letöltés: 2018.02.25.

²¹ ASIMOV, Isaac: Visit to the World’s Fair of 2014. The New York Times, August 16, 1964.

<http://www.nytimes.com/books/97/03/23/lifetimes/asi-v-fair.html>; letöltés: 2018.03.02.

²² STATISTA 3. Data volume of global consumer IP traffic from 2015 to 2021 (in petabytes per month).

<https://www.statista.com/statistics/267202/global-data-volume-of-consumer-ip-traffic/>; letöltés: 2018.01.26.

létrejöhettek a gondolatok és a tudásmegosztás világméretű szabad, semleges és korlátlan fóruma. Ám a 21. század elején bekövetkezett radikális internetes átalakulások, a közösségi hálózatok mindent elsőpró ereje, a hamis hírek, áltudományos sarlatánságok özöne – nem beszélve a kiberbűnözés, kiberhadsergek, trollok és zsarolóvírusok elterjedéséről – csúnyán szétzúzták és beárnyékolta az alapítóatya jóhiszemű idealista elképélését.²³

Az internet világa mindössze bő három évtized alatt létrehozta a több száz milliárd dollár forgalmat bonyolító webalapú kereskedelmet, a globális adathalászt és kereső szoftvereket, digitális oktatási platformokat és a világ népességének harmadát elérő közösségi hálózatokat, amelyek napjainkra az elsődleges információforrásokká és véleményformálók, vagy akár forradalom-előkészítő tényezőkké váltak emberek százmillióinak életében. Természetesen a napos oldal mellett ugyancsak megjelent az online kibertér alvilága, a TOR²⁴ programmal elérhető mély web (deep web) és annak a legvisszataszítóbb, illegális bűntanyája, a sötét web (dark web), amelynek oldalain az elemzések szerint mintegy 80%-ban gyomorforgató hardcore pedofil tartalmak, továbbá drog-, fegyver- és emberiszerv-kereskedelem vagy felforgató politikai agitáció, állam- és társadalomellenes terrorpropaganda zajlik²⁵ (2. kép).



2. kép. A web népszerű modellje²⁶

²³ SOLON, Olivia: Tim Berners-Lee on the future of the web: 'The system is failing'. The Guardian, 16 Nov 2017. <https://www.theguardian.com/technology/2017/nov/15/tim-berners-lee-world-wide-web-net-neutrality>; letöltés: 2018.01.29.

²⁴ The Onion Router (TOR) – (a hagymaszerver: háromszoros titkosítású 2. generációs elosztó program) az amerikai tengerészgyalogság kutatólaboratóriuma által 1997-ben kifejlesztett és ma már az Electronic Frontier Foundation által kezelt nyílt forráskódú szoftver a mély webes platformok, tartalmak eléréséhez.

²⁵ CHEN, Hsinchun: Dark Web: Exploring and Data Mining the Dark Side of the Web. Springer, New York, 2012.

²⁶ <http://deepwebtechblog.com/wp-content/uploads/2015/05/Deep-Web-Iceberg-e1432663755280.jpg>; letöltés: 2018.03.10.

A szingularitás hajnalán

A tudományos elméletet a napi valóság gyakorlatába vetítve a 21. századi okos tárgyak internetes világhálózatának témája, továbbá a mesterséges intelligenciát hordozó ember nélküli okoseszközök hadászati vagy polgári alkalmazásának kérdésköre igencsak komoly vitatéma a világ vezető hatalmai és a politikai, tudományos közvélemény számára egyaránt. Ezen a ponton különösen tetten érhető témaválasztásunk interdiszciplináris jellege és össztársadalmi fontossága, hiszen a kibertér és az összekapcsolt okoseszközök sokasága a modern társadalmi és gazdasági létünk minden szegmensét meghatározza és áthatja, következésképpen a kibertérben zajló folyamatok, jelenségek, lehetőségek és veszélyforrások biztonságpolitikai, gazdaságpolitikai és sok más egyéb vonatkozással bírnak. Ebből a nézőpontból elutasítandó és nehezen érthető a természettudósok és a számítástechnikai szakemberek gyakori nehezítése az egyéb tudományterületek képviselői irányába – vagy különösebben a hadtudományi és a biztonságpolitikai szakértők felé –, hiszen nyilvánvaló módon a kibertérben zajló számítógép-alapú történések már évtizedek óta nem csupán a rendszerfelügyelő mérnökök, új alkalmazásokat kialakító szoftverfejlesztő vagy károkozó programok vírusirtásával foglalkozó kiberbiztonsági szakemberek szakmai privilégiuma.

A társadalmi, gazdasági és katonai vonatkozások tekintetében a kibertér és a mesterséges intelligencia fejlődése hadtudományi, közgazdaságtani és nem utolsósorban filozófiai probléma is egyben, hacsak pusztán arra az egyszerű, de megválaszolatlan kérdésre gondolunk, hogy vajon az emberiség javára vagy inkább kárára válik a virtuális világ eszközeinek általános használata. Mi történik majd az emberiséggel, ha bekövetkezik az MI szingularitása, laikus módon egyszerűsítve: az emberi elme és a mesterséges elme szintbe kerülése? Vajon igaza lesz a számítógéptervező matematikus Neumann Jánosnak, illetve sci-fi írással is foglalkozó kollégájának, Vernor Vinge-nek, akik már az 1950-es években a technológiai és a számítógépes forradalmi paradigmaváltásról – technológiai szingularitásról – értekeztek, amely ha bekövetkezik – várhatóan a 21. század közepe táján –, akkor szerintük az emberiség által ismert történelem véget érhet?²⁷ E kérdések a hidegháború éveiben még nem váltottak ki túl nagy intellektuális vagy biztonságpolitikai érdeklődést, többnyire túl elméletinek, hipotetikusnak, illetve fantasztikusnak tartották a problémafelvetést. Nem úgy, mint napjainkban, amikor már a mesterséges intelligencia és a kibertér gazdasági, tudományos, továbbá katonai, politikai fontossága megkerülhetetlen tényezővé vált. Gondoljunk csak az IBM Watsonjára, a Google DeepMind-jára, az Apple Siri-jére, a hírhedt kibertroll-seregekre, a világhíres Sophiera, az első – szaúd-arábiai – humanoid robot állampolgárra (3. kép), nem is beszélve a takarító, felszolgáló, segítő japán háztartási robotokról, valamint az amerikai gyilkos drón repülőgépekről, harci robotkutyákról és mini robot aknakeresők seregéről. Itt érdemes megjegyeznünk, hogy a Sophiehoz hasonlóan a közeljövőben tömegesen előállított értelmes robotok, kiborgok léte nem várt jogi, nyelvészeti és filozófiai kérdéseket is felvet.

²⁷ VINGE, Vernor: Technological Singularity. Whole Earth Review, January 2003. http://cmm.cenart.gob.mx/delanda/textos/tech_sing.pdf; letöltés: 2018.02.26.

Nevezetesen, milyen jogokkal, státussal bír majd egy intelligens robot, illetve milyen névmással, jelzővel lehet vagy kell majd őt/azt illetni? Az MI és a robotmunkaerő elterjedése munkaerőpiaci és szociálpszichológiai hatásairól még talán korai következtetéseket levonni, mindenesetre nagyon komoly drasztikus következményekkel és feszültségekkel fog járni a 21. század társadalmában egy újabb okoseszköz-pusztító, gépromboló neoluddita²⁸ mozgalom kibontakozásának esélyeivel. A robotika és az MI társadalmi, munkaerőpiaci következményeiről számos és sokféle elképzelés született már. Martin Ford szerint²⁹ az általános alapjövedelem bevezetése az állampolgárok számára megoldást jelenthetne az általános társadalmi feszültséget generáló helyzet feloldására a közeljövőben.



3. kép. Sophie, az első igazi humanoid robot³⁰

A mesterséges intelligencia és a szingularitás témakörének talán legismertebb képviselője és internetes guruja, az amerikai Ray Kurzweil szerint – aki amúgy a Google műszaki igazgatója és a Szilikon-völgyben működő Szingularitás Egyetem³¹ társalapítója is egyben – a jelenlegi fejlődési trendeket tekintetbe véve 2029-re várható, amikor az első MI-eszköz sikeresen teljesíti a híres Turing-tesztet.³² Továbbá 2045-re ez már tömegesen is bekövetkezhet, ami egyenértékű lesz a technológiai MI-áttöréssel, vagyis a sokat említett szingularitással, és annak egyelőre még beláthatatlan következményeivel.³³

²⁸ Az 1810-es évek angol textilipari gyári munkás géprombolók modern megfelelői az okosrobotok ellen lázadva munkahelyeik védelmében.

²⁹ FORD, Martin: Robotok kora. HVG, Budapest, 2017.

³⁰ <https://www.dailydot.com/wp-content/uploads/600/7a/7670b9fcc31a0ad9-2048x1024.jpg>; letöltés: 2018.03.10.

³¹ Singularity University (Szingularitás Egyeteme) honlapja. <https://su.org/about/>; letöltés: 2018.02.22.

³² Alan Turing, a híres angol kódfejtő matematikus 1950-ben megalkotta az ember-gép ötperces, kérdésalapú intelligenciatesztjét.

³³ GALEON, Dom – REEDY, Christianna: Kurzweil Claims That the Singularity Will Happen by 2045. Futurism, October 5, 2017. <https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045/>; letöltés: 2018.02.22.

A humán elvészése miatt jogosan aggodalmaskodó, többnyire konzervatív gondolkodók szerint az emberiség önpusztító módon veszélyes és etikátlan kísérletbe kezdett, amikor tulajdonképpen önmagunkat akarjuk lélektelen, ellenben nagyon intelligens tökéletes gépekben reprodukálni, újratemetni.³⁴ Létre kívánjuk hozni a tökéletes egydimenziós műembert, amely lélektelen, mechanikus módon gondolkodva végrehajtja parancsainkat az asimovi robotika alaptörvényei szerint, de rögtön adódik a kérdés, hogy mi történik, ha – akarva-akaratlanul – porszem vagy programozási logikai hiba (szakszóval bug) kerül a vezérlőprogramba, az MI-rendszerbe, és mondhatni prométheuszi módon a tökéletes gépmember az alkotója ellen fordul? Habár a felvetés jelenleg még túl hipotetikusnak tűnhet, de az öntanuló gépek és az MI robbanásszerű exponenciális fejlődésével a probléma valószínűsége és realitása egyre növekszik. Gondolhatjuk, hogy a kibertérben történő folyamatokkal és a potenciális MI-alapú veszélyforrásokkal maguk a tervezők és a jövőbe látó filozófus-mérnökök lehetnek leginkább tisztában. Ezt a felvetést látszik erősíteni az a nyílt levél is, amelyet 2015 júliusában 26 ország 120 kimagasló globális technológiai cég vezetője, főmérnöke, szoftverfejlesztője közzétett – köztük Elon Musk, a Space X–Teslától és Mustafa Suleymannal, az Alphabet, a Google-t is birtokló anyacég elnökével – a világ vezetői és az ENSZ részére címezve az önjáró, ember nélküli gyilkos robotok és MI-hordozó pusztító eszközök betiltása érdekében.³⁵

Ismerve a vérzivataros emberi történelmet és az immanensen bennünk lévő teremtető és pusztító hajlamot, a fenti számítógépes guruk és MI-fejlesztő cégvezetők rettentő veszélyt és jövőbeli konfliktusforrást látnak ezen eszközök hadászati fejlesztésében és tömeges alkalmazásában, különösképpen emberek ellen. Nyilvánvalóan a versengő államok és legfőképp a terrorista csoportok, minden létező, beszerezhető eszközt hajlandóak fegyverként felhasználni céljaik elérése, érdekeik érvényesítése érdekében. Ezzel vállalják annak kockázatát, hogy az új halálos okoseszköz akár saját pusztulásukat is eredményezheti, amint azt szemléletesen bemutatja a Terminátor 5 című világhírű film Arnold Schwarzenegger és az öntudatra ébredő Skynet harcában. Sajnálatos módon ez az igencsak disztópikus forgatókönyv már nem csupán a valóságtól elrugaszkodott sci-fi filmek világába tartozik, hanem, amint már sokan – Neumann János, Vernor Vinge vagy Molnár Tamás mellett – közvetve utaltak rá, a holnaputáni valóságunk egyik lehetséges verziója. Ezért mindenképp szükséges és fontos döntés lenne az emberiség politikai és technológiai vezetői részéről a megfelelő technológiai óvintézkedések, elővigyázatos jogi és egyéb lépések fogantatása a mesterséges intelligencia és a milliárdnyi összekapcsolt okoseszköz ellenőrzése, irányítása és kizárólag békés célú felhasználása érdekében.

Természetesen nemcsak a kifinomult gondolkodású filozófusok és a humanitást is értékelő megszállott kiberszakértők, hanem a döntéshozó politikusok és a világtrendekre odafigyelő államfők is érzékelik az idők változását, valamint az új ipari forradalom kihívásait. Ezért nem meglepő, hogy Vladimir Putyin, az Oroszországi Föderáció elnöke 2017 októberében Szocsiában a 14. Valdaj nemzetközi

³⁴ MOLNÁR Tamás: *Én, Symmachus – Lélek és gép*. Európa Könyvkiadó, Budapest, 2000. pp. 194–199.

³⁵ Angol eredetiben UAK: unmanned autonomous killer robots. GIBBS, Samuel: Elon Musk leads 116 experts calling for outright ban of killer robots. *The Guardian*, 20 Aug 2017. <https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war>; letöltés: 2018.03.10.

üzleti fórumon a kibontakozó új világtrendről tartott előadásában kifejtette, hogy az az ország fogja uralni és irányítani a globális folyamatokat a 21. században, amelyik képes maximálisan kihasználni és irányítani a mesterséges intelligenciát.³⁶

A globális versengés és geopolitikai érdekszféra-konfliktus felfűzhető a Kína–Amerikai Egyesült Államok–Oroszország–Európai Unió főtengelyen, amely leginkább a fentebb hangoztatott békés célú és tudományos elvekkel ellentétben az új MI-alapú technológiák hadászati, kibervédelmi és gazdasági előnyszerzés céljából való hasznosításában mutatkozik meg. Az MI kutatásába-fejlesztésébe fektetett humán és pénzügyi tőke polgári és kormányzati célú felhasználása igencsak éles versengést mutat elsősorban a robotika, a kibernetika és az MI-kutatásban úttörő Amerikai Egyesült Államokban a szilikon-völgyi agytrösztök és kutatóközpontok, valamint a NASA és a hadügyminisztérium első számú kutató-fejlesztő ügynöksége, a híres-neves DARPA³⁷ között. Az orosz és a kínai MI-kutatás elsősorban hadászati, védelmi célú tudományos kutatóműhelyekben zajlik, míg Európában sajátos módon többnyire kisebb önálló, koordinálatlan egyetemi kutatócsoportok végzik ezt a fontos tudományos kutató-fejlesztő tevékenységet, jócskán elmaradva az amerikai társaiktól. A félmilliárd lakossal rendelkező Európai Unió, amely deklarálta 2020-ra világ legfejlettebb tudásalapú társadalmát szeretné létrehozni (egyre kevesebb eséllyel, sajnos), az Európai Kutatási Övezet (European Research Area) és a SPARC robotikafejlesztési programjában³⁸ a hétéves pénzügyi ciklusban évente mindössze 11 milliárd eurót szán interdiszciplináris tudományos kutatásra, amelyből körülbelül 2 milliárd euró jut a mesterséges intelligenciát célzó projektekre. Mindeközben a 340 milliós lélekszámú, viszont nagyon innovatív és kevésbé bürokratikus Amerikai Egyesült Államokban évente 180–250 milliárd dollárt költenek állami és magán vállalkozói forrásokból ugyanerre a kiemelt tudományos-technológiai területre, amit az Országos Tudományos és Műszaki Tanács (NSTC) 2016 májusában létrehozott Hálózat és Információs Technológiák Kutatás-Fejlesztési Albizottsága (NITRDSC) koordinál.³⁹ Európában a legtöbb egy főre jutó MI-alkalmazást használó vagy kutató cég – érdekes módon – az EU-n kívüli államban, ugyanakkor a legnagyobb európai tudományos központnak, a CERN-nek is helyet adó Svájcban található.⁴⁰

A feltörekvő Kínában 2015-tel kezdődően évente 7–10 milliárd dollárnyi keretösszeget fordítanak MI-alapú kutatás-fejlesztési projektekre, de a valóságban a hadászati célú titkos projektekkal kiegészülve ez a keretszám jóval magasabb lehet. Kína kinyilvánított ambíciózus célja, hogy 2030-ra az Amerikai Egyesült Államokat megelőzve a világ vezető MI-kutató és -alkalmazó országa legyen, ezért Peking

³⁶ Meeting of the Valdai International Discussion Club, October 19, 2017. <http://en.kremlin.ru/events/president/news/55882>; letöltés: 2018.02.22.

³⁷ Defense Advanced Research Projects' Agency – Fejlett Védelmi Kutatási Projektek Ügynöksége.

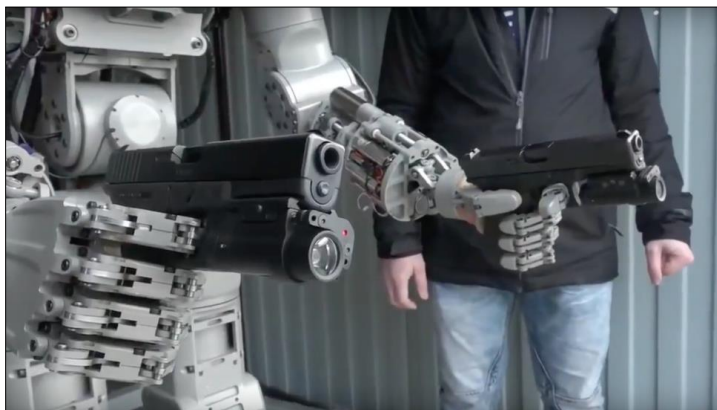
³⁸ ANSIP, Andrus: Making the most of robotics and artificial intelligence in Europe. European Commission, 17 November 2017. https://ec.europa.eu/commission/commissioners/2014-2019/ansip/blog/making-most-robotics-and-artificial-intelligence-europe_en; letöltés: 2018.03.10.

³⁹ The National Artificial Intelligence Research and Development Strategic Plan. NSTC NITRD, October 2016. https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf; letöltés: 2018.02.28.

⁴⁰ The European Artificial Intelligence Landscape More than 400 AI companies built in Europe. City. AI, Jul 30, 2017. <https://medium.com/cityai/the-european-artificial-intelligence-landscape-more-than-400-ai-companies-build-in-europe-bd17a3d499b>; letöltés: 2018.03.05.

mellett létrehozzák Ázsia legnagyobb, 55 hektáros MI-kutatóbázisát 2,2 milliárd dollárból,⁴¹ ahol elsősorban a gépi tanulási (deep/machine learning) folyamatokat, felhőszolgáltatásokat (cloud computing) és nagybani adatelemzést (big data) fogják kutatni, fejleszteni több tízezer válogatott szakemberrel.

Az új okos technológiák hadászati célú felhasználását vizsgáló szakemberek, valamint a kibbiztonsággal foglalkozók érdeklődését is igencsak izgatja a nagyfokú orosz titkolózás ebben a tekintetben, hiszen nyilvánosan csak a Yandex nevű internetes óriás cég kutatócsoportja és a Kazanyi Állami Tudományegyetem Gépi Tudatosság Kutatólaboratóriuma foglalkozik tudományos jellegű MI-kutatással Oroszországban. Ahogy Elon Musk, az úttörő technológiák világszerte ismert magánvállalkozója megjegyezte,⁴² a nagyon fejlett és kifinomult technológiákat alkalmazó orosz hadiipar ismeretében, gyanakvásra és aggodalomra adhat okot – különösen Putyin elnök célzott kijelentéseinek fényében –, hogy az orosz MI-kutatásról nem sok megbízható információval rendelkezünk. Mindez arra enged következtetni, hogy valójában az oroszok gőzerővel folytatnak ezirányú titkos fejlesztéseket, kutatásokat, mint például a büszkén bemutatott híressé vált FEDOR robot,⁴³ amely nemcsak autót, de akár az új orosz űrkompot is képes lesz elvezetni, ellenben – sajátosan orosz módra – mintegy Terminator-szerűen pisztollyal a kezében jelent meg 2017-ben (4. kép).



4. kép. FEDOR, az első orosz robot⁴⁴

Nyilvánvaló stratégiai okokból egyetlen nagyhatalom sem engedheti meg magának, hogy lemaradjon a fentiekhez hasonló, forradalmian új technológiák és korszerű nem hagyományos fegyvernemek fejlesztéséből és gyakorlati alkalmazásából.

⁴¹ CYRANOSKI, David: China enters the battle for AI talent. Nature, 15 January 2018. <https://www.nature.com/articles/d41586-018-00604-6> letöltés: 2018.03.07.

⁴² BERSHIDSKY, Leonid: Take Elon Musk Seriously on the Russian AI Threat. Bloomberg, 2017.09.05. <https://www.bloomberg.com/view/articles/2017-09-05/take-elon-musk-seriously-on-the-russian-ai-threat>; letöltés: 2018.03.01.

⁴³ O'CONNOR, Tom: U.S. Is Losing To Russia And China In War For Artificial Intelligence, Report Says. Newsweek, 11/29/17. <http://www.newsweek.com/us-could-lose-russia-china-war-artificial-intelligence-726603>; letöltés: 2018.03.02.

⁴⁴ <https://nerdist.com/wp-content/uploads/2017/06/FEDOR-Feature-Image-06212017.jpg>; letöltés: 2018.03.08.

Sokak szerint a globális méretű világháború már 2007. április 27-én elkezdődött az Észtország elleni összehangolt túlterheléses botnet kibertámadással,⁴⁵ amelyet a szakírók már csak az első kiberháborúnak (Web War I.) neveznek.⁴⁶ A közel egy héten keresztül zajló kibertámadás a mintegy másfél millió lakosú balti ország életét teljesen megbénította, mivel leállította a távközlési, a banki, valamint a közlekedési informatikai rendszereket. A „szovjet bronzkatona éjszakáját” követő példátlan erejű, demonstratív kibertámadás-sorozat digitális lábnyomai oroszországi szerverekhez vezettek, bár az orosz kormányzat természetesen mindenféle érintettséget és beavatkozást hevesen és indulatosan tagadott a szomszédos parányi EU- és NATO-tagállammal szemben.

Az utóbbi évtizedben nagyon elszaporodtak a hasonló jellegű, de kisebb intenzitású kibertámadások a világban. Államok és óriás üzleti társaságok próbálnak előnyös pozíciókat, lehetőségeket kiharcolni saját maguk részére a kibertér szabályok és határok nélküli harcmezéjén. Talán ezért is mondta Toomas Hendrik Ilves, volt észt elnök kiberbiztonságot is érintő beszédében, hogy az európai politikus döntéshozók még mindig nem nagyon értik, vagy nem akarják tudomásul venni a kibertér biztonságpolitikai, gazdasági és katonai jelentőségét, például az amerikaiakkal és az oroszokkal ellentétben.⁴⁷ A digitalizáció gyors előretörése előtti korban szocializálódott politikai és katonai vagy hírszerzési döntéshozók hajlamosak lebecsülni vagy nem megfelelő súllyal és fontossággal kezelni a kiber- és az MI-alapú technológiákat, alkalmazásokat, aminek nagyon komoly és akár tragikus következményei is lehetnek. Elég, ha csak az örült norvég tömeggyilkos Breivikre vagy a párizsi Bataclan klubban vérontást rendező belga terroristákra gondolunk, akik mindannyian a többszereplős online stratégiai harci játékok⁴⁸ belső, zárt, titkosított kommunikációs csatornáin egyeztettek akcióikat vagy könnyedén beszerezték illegálisan lőfegyvereiket.⁴⁹

Összegzés

Napóleon, a modern történelem egyik legnagyobb hadvezére is felismerte, hogy az eszmék és a szellem erejét nem szabad alábecsülni, mert hosszú távon legyőzik a kardot is, később hozzátéve, hogy tulajdonképpen a háború oroszlánrészt információból áll.⁵⁰ Mindkét gondolat, különösképpen két évszázad távlatából szembevető relevanciával rendelkezik és kimagasló helyzetfelismerésről, intellektuális éleslátásról tesz tanúbizonyságot, amelyek meghatározóak lehetnek egy ország vagy haderő sikeressége szempontjából.

⁴⁵ DDOS-attack avagy túlterheléses parancsmegtagadáson alapuló kibertámadás több tíz vagy százezer számítógép (zombigépek) összehangolt (botnetes) másodlagos háttérirányításával egy célpont ellen.

⁴⁶ Web War I. avagy az első webháború Észtország ellen, 2007. április 27-től május 2-ig. O'NEILL, Patrick Howell: The cyberattack that changed the world. The Daily Dot, May 20, 2016. <https://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/>; letöltés: 2018.03.08.

⁴⁷ SCHULTZ, Teri: A Decade after „Web War I,” Former Estonian President Blasts EU Cyber Inertia. Atlantic Council, April 26, 2017. <http://www.atlanticcouncil.org/blogs/new-atlanticist/a-decade-after-web-war-1-former-estonian-president-blasts-eu-cyber-inertia>; letöltés: 2018.03.02.

⁴⁸ Massive Multi-Player Online Battle Arena, First Person Shooter, Role Play Games mint League of Legends, World of Warcraft, World of Tanks stb.

⁴⁹ KIS-BENEDEK József: Dzsihadizmus, radikalizmus, terrorizmus. Zrínyi Kiadó, Budapest, 2016. p. 150.

⁵⁰ CITATUM: Bonaparte Napoleon-idézetek. https://www.citatum.hu/szerzo/Bonaparte_Napoleon; letöltés: 2018.02.26.

Napjainkban a kardnál erősebb eszme az évezredek óta újragondolt vallásos hit feltámadásában és a lehengerlő tudományos technikai felfedezések formájában jelentkezik. Az információ pedig a bennünket körülvevő fizikai és immár a virtuális valóságból is származó adatok, jelzések összessége. A modern számítógép-alapú technológiák meghatározzák életünket, és minél jobban kötődünk hozzájuk, annál inkább sérülékennyé, kiszolgáltatottabbá teszik a civilizációnkat és a globális gazdaságot egyaránt. Olyan új kommunikációs eszközök és csatornák jöttek létre, amelyekre az emberiség nem igazán tudott felkészülni egy-két emberöltő rövid időszávjá alatt, akárcsak hasonló módon az információs technológiák szélesebb fejlődésével sem képesek lépést tartani az információbiztonságot szolgáló elhárító, védekező technikák és alkalmazások. Ez a biztonsági és információs rés (security and intelligence gap) a felhasználó szándékától függően komoly előnyt vagy éppen hátrányt jelent akár egy nagy szuverén állam, vagy egy multinacionális, stratégiai gerinchálózatot működtető vállalat, vagy egy kiberfegyvernemhez tartozó katonai egység számára. Ennek pusztító hatását már megtapasztalhatták az észtek, a grúzok és a dél-koreaiak az országaik ellen 2007-ben, 2008-ban, illetve 2012-ben indított összehangolt kibertámadás-sorozatok idején.



5. kép. Robotjövő?⁵¹

Aszimmetrikus világunk súlypontja visszafordíthatatlanul eltolódni látszik a virtuális kibervilág irányába, annak minden pozitív és negatív hozadékaival egyetemben, és láthatóan ezt a folyamatot megállítani már nem, csupán lassítani lehet. A kibernetika, a robotika és a mesterséges intelligencia új felfedezései sokkal élhetőbbé és könnyebbé tehetik az emberek millióinak életét. Ugyanakkor mindezek a folyamatok ártó szándékú rövidlátó, önző célú vezetők és csoportosulások kezében akár egész civilizációnk veszét is okozhatják. Várhatóan a közeljövő katonai jellegű konfliktusai elsősorban a kiberhadszíntérben fognak lezajlani vagy kibontakozni, továbbá az önálló döntésekre képes intelligens harci eszközök alkalmazása

⁵¹ <http://www.benedict1.com/digitalartist/cyber-future/large/cyber-future20.jpg>; letöltés: 2018.03.10.

valószínűleg döntő szerepet fog játszani, ami a hadviselés egy teljesen új, ismeretlen horizontját nyithatja meg. Az infokommunikációs és az MI-kutató szakemberek, illetve a döntéshozók a megfelelő szakértelemmel és a régi bölcsék megfontolt óvatosságának (prudencia) és mértékletességének alkalmazásával az emberiség javára fordíthatják a páratlanul új forradalmi technológiákat (5. kép). Csupán az ősrégi senecai kérdést kell feltennünk és folyamatosan megválaszolnunk, hogy cui prodest, cui bono? Valójában kinek használ és kinek jó a számtalan új műszaki eszköz, robot és kiberalkalmazás? Ezekre a kérdésekre a jövő történései és társadalmi folyamatai fognak hamarosan válaszokat adni, és remélhetőleg nem kell majd felidézni a közhelyszerű bölcsességet, miszerint majdnem minden katasztrófa után eszünkbe jutnak a szakértők figyelmeztető szavai, akik előre szóltak, de nem vették őket figyelembe.

FELHASZNÁLT IRODALOM

- ANSIP, Andrus: Making the most of robotics and artificial intelligence in Europe. European Commission, 17 November 2017.
https://ec.europa.eu/commission/commissioners/2014-2019/ansip/blog/making-most-robotics-and-artificial-intelligence-europe_en; letöltés: 2018.03.10.
- ASIMOV, Isaac: Visit to the World's Fair of 2014. The New York Times, August 16, 1964.
<http://www.nytimes.com/books/97/03/23/lifetimes/asi-v-fair.html>; letöltés: 2018.03.02.
- BARABÁSI Albert-László: Behálózva – A hálózatok új tudománya. Helikon Kiadó, Budapest, 2013.
- BERSHIDSKY, Leonid: Take Elon Musk Seriously on the Russian AI Threat. Bloomberg, 2017.09.05.
<https://www.bloomberg.com/view/articles/2017-09-05/take-elon-musk-seriously-on-the-russian-ai-threat>; letöltés: 2018.03.01.
- CHEN, Hsinchun: Dark Web: Exploring and Data Mining the Dark Side of the Web. Springer, New York, 2012.
- CITATUM: Bonaparte Napoleon-idézetek.
https://www.citatum.hu/szerzo/Bonaparte_Napoleon; letöltés: 2018.02.26.
- CLARKE, Richard A. – Knake, Robert K.: Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins, New York, 2010.
- CLAUSEWITZ, Carl von: A háborúról. Zrínyi Kiadó, Budapest, 2013.
- CYRANOSKI, David: China enters the battle for AI talent. Nature, 15 January 2018.
<https://www.nature.com/articles/d41586-018-00604-6> letöltés: 2018.03.07.
- EVANS, Martin – Scott, Patrik: Fraud and cyber crime are now the country's most common offences. The Telegraph, 19 January 2017.
<https://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/>; letöltés: 2018.01.29.
- FORD, Martin: Robotok kora. HVG, Budapest, 2017.

- GALEON, Dom – REEDY, Christianna: Kurzweil Claims That the Singularity Will Happen by 2045. Futurism, October 5, 2017.
<https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045/>; letöltés: 2018.02.22.
- GETTY, Mark: Blood and Oil. The Economist, March 2, 2000.
<https://www.economist.com/node/288515>; letöltés: 2018.03.02.
- GIBBS, Samuel: Elon Musk leads 116 experts calling for outright ban of killer robots. The Guardian, 20 Aug 2017.
<https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war>; letöltés: 2018.03.10.
- GIBSON, William: Cyberspace.
<http://www.technovelgy.com/ct/content.asp?Bnum53>; letöltés: 2018.02.25.
- GULYÁS Attila: Kiberhadviselés észak-koreai módra II. Szakmai Szemle, XV. évfolyam 4. szám, 2017. december. pp. 30–42.
http://knbsz.gov.hu/hu/letoltes/szsz/2017_4_szam.pdf; letöltés: 2018.03.01.
- <http://deepwebtechblog.com/wp-content/uploads/2015/05/Deep-Web-Iceberg-e1432663755280.jpg>; letöltés: 2018.03.10.
- <http://www.benedict1.com/digitalartist/cyber-future/large/cyber-future20.jpg>; letöltés: 2018.03.10.
- <https://nerdist.com/wp-content/uploads/2017/06/FEDOR-Feature-Image-06212017.jpg>; letöltés: 2018.03.08.
- <https://pbs.twimg.com/media/DNZFrueWkAAKKRU.jpg>; letöltés: 2018.03.10.
- <https://www.dailydot.com/wp-content/uploads/600/7a/7670b9fcc31a0ad9-2048x1024.jpg>; letöltés: 2018.03.10.
- KAPLAN, Jerry: Artificial Intelligence: What Everyone Needs to Know. Oxford University Press, New York, 2016.
- KIS János: A régi görögök erköltséinek és szokásainak vagy vallásbéli, polgári, hadi és házi rendtartásainak leírása Eschenburg szerint. Wéber Simon Péter nyomdája, Pozsony, 1809. (Google e-könyv verzió)
- KIS-BENEDEK József: Dzsihadizmus, radikalizmus, terrorizmus. Zrínyi Kiadó, Budapest, 2016.
- KURZWEIL, Ray: Singularity is Near: When Humans Transcend Biology. Penguin Books, New York, 2006.
- Meeting of the Valdai International Discussion Club. October 19, 2017.
<http://en.kremlin.ru/events/president/news/55882>; letöltés: 2018.02.22.
- MOLNÁR Tamás: Én, Symmachus – Lélek és gép. Európa Könyvkiadó, Budapest, 2000.
- Norbert Wiener – Wikipédia szócikk.
https://hu.wikipedia.org/wiki/Norbert_Wiener; letöltés: 2018.01.19.
- O'CONNOR, Tom: U.S. Is Losing To Russia And China In War For Artificial Intelligence, Report Says. Newsweek, 11/29/17.
<http://www.newsweek.com/us-could-lose-russia-china-war-artificial-intelligence-726603>; letöltés: 2018.03.02.

- O'NEILL, Patrick Howell: The cyberattack that changed the world. The Daily Dot, May 20, 2016.
<https://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/>; letöltés: 2018.03.08.
- SCHULTZ, Teri: A Decade after „Web War 1,” Former Estonian President Blasts EU Cyber Inertia. Atlantic Council, April 26, 2017.
<http://www.atlanticcouncil.org/blogs/new-atlanticist/a-decade-after-web-war-1-former-estonian-president-blasts-eu-cyber-inertia>; letöltés: 2018.03.02.
- Singularity University (Szingularitás Egyeteme) honlapja.
<https://su.org/about/>; letöltés: 2018.02.22.
- SOLON, Olivia: Tim Berners-Lee on the future of the web: 'The system is failing'. The Guardian, 16 Nov 2017.
<https://www.theguardian.com/technology/2017/nov/15/tim-berners-lee-world-wide-web-net-neutrality>; letöltés: 2018.01.29.
- STATISTA 1. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions).
<https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>; letöltés: 2018.01.28.
- STATISTA 2. Global digital population as of April 2018 (in millions).
<https://www.statista.com/statistics/617136/digital-population-worldwide/>; letöltés: 2018.02.25.
- STATISTA 3. Data volume of global consumer IP traffic from 2015 to 2021 (in petabytes per month). <https://www.statista.com/statistics/267202/global-data-volume-of-consumer-ip-traffic/>; letöltés: 2018.01.26.
- SULLEYMAN, Aatif: Roobot being trained to shoot guns is 'not a terminator' insists Russian Deputy Prime Minister. Independent, 14 April 2017.
<http://www.independent.co.uk/life-style/gadgets-and-tech/news/terminator-robot-fedor-guns-russia-shooting-dmitry-rogozin-a7684406.html>; letöltés: 2018.02.28.
- The European Artificial Intelligence Landscape More than 400 AI companies built in Europe. City.AI, Jul 30, 2017.
<https://medium.com/cityai/the-european-artificial-intelligence-landscape-more-than-400-ai-companies-build-in-europe-bd17a3d499b2>; letöltés: 2018.03.05.
- The National Artificial Intelligence Research and Development Strategic Plan. NSTC NITRD, October 2016.
https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf; letöltés: 2018.02.28.
- TOONDERS, Joris: Data Is the New Oil of the Digital Economy. Wired, July 2014.
<https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/>; letöltés: 2018.01.25.
- VINGE, Vernor: Technological Singularity. Whole Earth Review, January 2003.
http://cmm.cenart.gob.mx/delanda/textos/tech_sing.pdf; letöltés: 2018.02.26.